IN THE CLAIMS

1. (Previously presented) Apparatus for secure management of data in a computer controlled storage system comprising:

a trusted data management server (tdm server), responsive to a user or user program application, capable of storing data in and retrieving data from a storage system that comprises:

security structure generator means to generate the following security management structures:

a unique identifier for said data;

access control information for said data;

a data signature for authenticating said data from said data and said unique identifier; and

an access control information signature for authenticating said access control information from said access control information and said unique identifier.

2. (Previously presented) The apparatus of claim 1 further comprising:

encryption means for encrypting:

said data; and

said access control information, when required by said tdm server.

3. (Original) The apparatus of claim 2 wherein said encryption means is adapted to encrypt said data and said access control information.

4. (Previously presented) The apparatus of claim 2 further comprising:

storage control means for causing said storage system to store said security management structures and said data.

5. (Original) The apparatus of claim 4 wherein said data is stored in encrypted form.

6. (Previously presented) The apparatus of claim 5 further comprising:

access control means for accessing said data stored in said storage system with said unique identifier

7. (Previously presented) The apparatus of claim 6 wherein said access control means comprises:

means responsive to a request from ~~an~~ a user for accessing secured data from said storage system, adapted to:

retrieve a unique identifier for said data from said user or storage system;

retrieve from said storage system said security management structures corresponding to said data; and

carry out the following determination steps:

determine if said access control information and unique identifier correspond with said access control information signature;

determine if said data and its unique identifier correspond with said data signature;

determine if said unique identifier of said access control information corresponds with said unique identifier of said secured data; and

determine whether said access control information permits said user to access said secured data; and then grant access to said user to said data if each of said determination steps is satisfied, and otherwise refuse access.

8. (Original) The apparatus of claim 7 wherein said access control means further includes means to notify said user if access is refused.

9. (Original) A system for secure management of data in a computer controlled storage system comprising:

a trusted data management server (tdm server) accessible to a user or user program application;

storage means managed by a storage server;

a communication system for connecting said trusted data management server and said storage server for the transfer of information therebetween;

said tdm server being adapted to manage protected data in said storage means with unique identifiers, data signatures, access control information, and access control information signatures;

said storage server being adapted to store protected data, signatures of said data, unique identifiers, access information, access information signatures , to permit access of said protected data under management of said tdm server.

10. (Original) A system for the secure management of documents in a database system comprising:

a trusted document management server (tdm server) accessible to a user or user program application;

database storage managed by a database server (db server);

a communication system for communicating between said trusted document management server and said database server;

wherein said tdm server is adapted to handle requests for managing protected documents in said database with unique identifiers and access control information; and

wherein said db server is adapted to store protected documents, signatures of the documents, unique identifiers and access information, signature of said access information, to permit access of said protected documents under management of said tdm server.

11. (Previously presented) The system of claim 10 wherein: on the request of a user to create and store a protected document in said database storage,

said tdm server is adapted:

to generate one or more random identifiers and request that said db server reserve one of said random identifiers as a unique identifier for said document;

to compute a signature of said document which authenticates a predetermined set of attributes including document content, and said unique identifier for said document;

to create access control information in the form of an access control list;

to compute a signature of said access control list which authenticates a predetermined set of attributes including the access control information content, and said unique identifier for said document; and,

to have said database server store in said database, said document in protected form, its signature, said access control list and said signature of said access control list;

wherein said database server is adapted to verify whether said random identifier does not correspond to a unique access number of any other protected document, and if so, to reserve it.

12. (Previously presented) A method for secure management of data in a computer controlled storage system comprising:

in a trusted data management server (tdm server), responsive to a user or user program application, for storing data in and retrieving data from a storage system generating the following security management structures:

a unique identifier for said data;

access control information for said data;

a data signature for authenticating said data from said data and said unique identifier; and

an access control information signature for authenticating said access control information from said access control information and said unique identifier.

13. (Original) The method of claim 12 further comprising:

encrypting said data, or said access control information.

14. (Original) The method of claim 13 comprising encrypting said data and said access control information.

15. (Previously presented) The method of claim 13 further comprising:
causing said storage system to store said security management structures and said data.

16. (Original) The method of claim 15 wherein said data is stored encrypted

17. (Original) The method of claim 16 further comprising:
accessing said data stored in said storage with said unique identifier

18. (Previously presented) The method of claim 16 responsive to a request from a user for accessing data from said storage system, retrieving a unique identifier for said data from said user or database storage;

retrieve from said storage system said security management structures corresponding to said secured data; and

carrying out the following determination steps:

determine if said access control information and its unique identifier correspond with said access control information signature;

determine if said secured data and its unique identifier correspond with said data signature;

determine if said unique identifier of said access control information corresponds with said secured data; and

determine whether said access control information permits said user to access said secured data; and then granting access to said user to said data if each of said determination steps is satisfied, and otherwise refusing access.

19. (Original) The method of claim 18 including notifying said user if access is refused.

20. (Original) In a system for secure management of data in a computer controlled storage system comprising:

a trusted data management server (tdm server) accessible to a user or user program application;

storage means managed by a storage server;

a communication system for connecting said trusted data management server and said storage server for the transfer of information therebetween;

using tdm server to manage protected data in said storage means with unique identifiers, data signatures, access control information, and access control information signatures;

and storing in said storage means protected data, signatures of said data, unique identifiers, access information, access information signatures, to permit access of said protected data under management of said tdm server.

21. (Original) In a system for the secure management of documents in a database system comprising:

a trusted document management server (tdm server) accessible to a user or user program application;

database storage managed by a database server (db server);

a communication system for communicating between said trusted document management server and said database server;

using said tdm server to handle requests for managing protected documents in said database by using unique identifiers and access control information; and

storing in said database storage protected documents, signatures of the documents, unique identifiers and access information, signature of said access information, to permit access of said protected documents under management of said tdm server.

22. (Original) In the system of claim 21 wherein: on the request of a user to create and store a protected document in said database, said tdm server generates one or more random numbers and request that said db server reserves one of said random numbers as a document access key;

computes a signature of said document which authenticates a predetermined set of attributes including document content, and said document key;

creates access control information in the form of an access control list;

computes a signature of said access control list which authenticates a predetermined set of

attributes including the access control information content, and said document key; and, has said database server store in said database, said document in protected form, its signature, said access control list and said signature of said access control list.

23. (Previously presented) Computer readable storage means for storing instructions for use in the execution in a computer system of the method of claim 13.

24. (Previously presented) Computer readable storage means for storing instructions for use in the execution in a computer system for causing the computer system to effect the apparatus of claim 1.

25. (Previously presented) Computer readable storage means for storing instructions for use in the execution in a computer system for causing the computer system to effect the system of claim 9.

26. (Previously presented) Computer readable storage means for storing instructions for use in the execution in a computer system for causing the computer system to effect the system of claim 10.

27. (Previously presented) An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing secure management of data in a computer controlled storage system, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 12.

28. (Previously presented) Computer readable storage means for storing instructions for use in the execution in a computer system for causing a computer system to effect the system of claim 20.

29. (Previously presented) Computer readable storage means for storing instructions for use in the execution in a computer system for causing a computer system to effect the system of claim 21.

30. (New) A method for storing a document in a secure storage system comprising the steps of:

submitting the document for secure storage;

generating a random number at a trusted document management server;

requesting a database management system to reserve the generated random number as a document key;

computing a digital document signature at the trusted document management server, wherein the document signature is capable of authenticating document content and the document key;

creating an initial access control list (ACL) at the trusted document management server;

computing a digital ACL signature at the trusted document management sever, wherein the ACL signature is capable of authenticating ACL content and the document key; and

instructing the database management system to store the document, the document signature, the ACL and the ACL signature.

31. (New) A method for retrieving a protected document from a secure storage system comprising the steps of:

submitting a request from a user for retrieval of the document;

obtaining a document key;

retrieving an access control list (ACL) of the document and an ACL signature;

determining if the retrieved ACL corresponds to the retrieved ACL signature;

rejecting retrieval of the protected document when the retrieved ACL does not correspond to the retrieved ACL signature;

retrieving the protected document and the document signature from a database management system when the retrieved ACL corresponds to the retrieved ACL signature;

determining if protected document corresponds to the document signature;

rejecting retrieval of the protected document when the protected document does not correspond to the document signature;

determining if a document key authenticated by the document signature corresponds to a document key authenticated by the ACL signature when the protected document corresponds to the document signature;

rejecting retrieval of the protected document when the document key authenticated by the document signature does not correspond to the document key authenticated by the ACL signature; and

using the ACL to determine user access to the protected document when the document key authenticated by the document signature corresponds to the document key authenticated by the ACL signature.